UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,952	12/11/2000	Aravind Sitaraman	CISCO-3294	4939

7590 04/15/2004

EXAMINER
PATEL, ASHOKKUMAR B

ART UNIT	PAPER NUMBER
2154	6

David B. Ritchie
Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164-0640

DATE MAILED: 04/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/734,952	SITARAMAN ET AL.	
	Examin r	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this c mmunication appears n the cover she t with the c rrespondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-45 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-45 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Application Number 09/734, 952 was filed on 12/11/2000. Claims 1-45 are subject to examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 12, 23, 34 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Prabandham et al. (hereinafter Prabandham)(US 6,701,438).

Referring to claim 1,

The reference teaches a method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers (A servlet engine that includes a security module that assures that only those requests that are properly authenticated and authorized are serviced by a servlet. (Abstract)), comprising:

- receiving a HTTP request from a subscriber using a first communication network (Fig.2, elements 202 making http request to element 204), coupled to at least one other communication network (Fig. 2, element 206), said request including a Universal Resource Locator (URL) (col. 4, lines 19-31);

- receiving a profile for said subscriber; filtering said request to determine whether said subscriber is authorized to make said request based upon said profile; (col.4, lines 65-67); and

- forwarding said request to said at east one other communication network when said subscriber is authorized to make said request. (col.4, line 67 and col. 5, lines 1-8).

Referring to claim 12,

Claim 12 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the method of claim 1. Therefore, claim 12 is rejected for the reasons set forth for the claim 1.

Referring to claim 23,

Claim 23 is a claim to an apparatus carrying out the method of claim 1. Therefore, claim 23 is rejected for the reasons set forth for the claim 1.

Referring to claim 34,

The reference teaches an apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers (A servlet engine that includes a security module that assures that only those requests that are properly authenticated and authorized are serviced by a servlet. (Abstract)), said apparatus comprising:

- a profile request generator capable of generating a profile request based upon a HTTP request received from a subscriber using a first communication network (Fig.2, elements 202 making http request to element 204), said request including a Universal Resource Locator (URL)(col. 4, lines 19-31);

- a filter capable of determining whether said request is authorized based upon said requested profile; and (Fig. 2, element 212, col.4, lines 65-67);

- an authorizer capable of allowing said request said request to be forwarded on at least one other communication network coupled to said first communication network. (Fig. 2, element 216 and col.4, line 67 and col. 5, lines 1-8).

Referring to claim 35,

The reference teaches an apparatus comprising:

- a first receiving interface capable of accepting said request; (Fig. 1, element 212's receiving interface)

- a first forwarding interface capable of sending said profile request to an AAA server; (element 212 which has the first receiving interface which is AAA server)

- a second receiving inter-face capable of accepting a requested profile; and a second forwarding interface capable of forwarding said request on said at least one other communication network. (element 216's interfaces connected to element 212 and element 206)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2-11, 13-22, 24-33 and 36-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Prabandham et al. (hereinafter Prabandham)(US 6,701,438) in view of Primeaux et al. (hereinafter Primeaux) (US 6,334,121).

Referring to claim 2,

The reference Prabandham teaches HTTP request being made by the subscriber. (Fig. 2, element 202 making http request). The reference also teaches of a servlet engine that includes a security module that assures that only those requests that are properly authenticated and authorized are serviced by a servlet. (applying HTTP server attack preventative measures). A logging module provides customized records of both security module and servlet transactions (counts the HTTP requests and updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and.) (Abstract). The reference also teaches that the logging of the servlet transactions provide the capability of, for example, tracking hackers (both potential and actual) by logging multiple failed accesses by a particular browser within a specific period of time or determine the frequency and type of various security failures promulgated by the user of a particular browser. (col. 4, lines 60-64). The reference also teaches that the logging module typically tracks information related to IP (Internet Protocol) address information indicative of the virtual location of the browser 200 of Fig. 2, as well as the number of successful hits versus the number of unauthorized and/or unauthenticated requests posted to it by the security module 212 of Fig. 2. With this information, a developer is able to track the number and type of http requests which the servlet processes. (col. 5, lines 9-16). The reference fails to teach applying HTTP

server attack preventative measures when said request count exceeds a maximum HTTP request count. The reference Primeaux teaches a method that will prevent a destructive command from being executed. Several commands for each of the system users are tracked. A combination of security rules and user usage patterns are used to flag suspicious activity on the system. Security rules are centered around those types of commands that are potentially destructive in nature and take into account the user's normal level of access privileges. (col. 2, lines 45-52). The reference also teaches that the system also may have two or more threshold levels for security monitoring: one for normal operations and any number for heightened security. (teaches to set a threshold level of normal operations such as request count exceeding a maximum HTTP request count.)(col.3, lines 21-24). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's logging module's capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request counts set by the security rules of Primeaux. In this way, a web site owner is able to better track the web site usage as well as be able to determine the number of users which have attempted to enter a particular site and those that have failed and/or succeeded in entering the site in question as taught by Prabandham.

Referring to claims 3, 4 and 5,

Keeping in mind the teachings of Prabandham as stated above, although the reference teaches the packet switching protocols such as TCP exchanging messages between the subscriber and named host including a server (Fig. 1, col. 1, lines 20-37), the reference fails to teach setting an alarm when request count exceeds said maximum HTTP request count and sending alarm to an Internet Service Provider (ISP) associated with subscriber and, dropping the data packet containing request when said request count exceeds maximum HTTP request count. The reference Primeaux teaches the action taken could be defined to suspend the user account or merely mail a message to the system administrator (sending alarm to an Internet Service Provider (ISP) associated with subscriber), warning of a potential intruder including the category of users such as Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (dropping the data packet containing request). Various levels of security are determined by the list of commands deemed critical by the system administrator. (col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's logging module's capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive

measures based on the set threshold levels such as request count exceeding a maximum HTTP request counts set by the security rules and setting an alarm to the ISP (the system administrator) or dropping a packet containing the request when request count exceeds a maximum HTTP. This provides a system wherein the system will detect a difference in the pattern of command usage. When such a difference is detected, it will be compared to the set of security rules and the system will take the appropriate action.

Referring to claims 6, 7, 8, and 9,

Keeping in mind the teachings of Prabandham as stated above, although the reference teaches the subscriber and the first communication network (Fig.2, elements 202 making http request to element 204), the reference fails to teach shutting down the account used to access first communication network when request count exceeds said maximum HTTP request count and disabling HTTP requests for a hold-down period when request count exceeds maximum HTTP request count. The reference The reference Primeaux teaches the action taken could be defined to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) or merely mail a message to the system administrator, warning of a potential intruder including the category of users such as Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the

degree of destructiveness of a particular command and the level of security awareness that the software is set for (hold-down period each time HTTP count exceeds said maximum HTTP request count and hold-down period increases exponentially each time HTTP count exceeds maximum HTTP request count). Various levels of security are determined by the list of commands deemed critical by the system administrator. (col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's logging module's capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request counts set by the security rules and to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) as desired, based on the level of security awareness that the software is set for (hold-down period each time HTTP count exceeds said maximum HTTP request count and hold-down period increases exponentially each time HTTP count exceeds maximum HTTP request count) when request count exceeds a maximum HTTP. This provides a system wherein the system will detect a difference in the pattern of command usage. When such a difference is detected, it will be compared to the set of security rules and the system will take the appropriate action.

Referring to claims 10 and 11,

In addition to the teachings indicated above, the reference Prabandham's servlet handles those requests that are authenticated and authorized by the security module

and the servlet notifies the logging module of those requests which have been successfully handled by the servlet with a first type flag. The servlet notifies the logging module of those requests which have not been successfully handled by the servlet with a second type flag. (col.2, lines 53-60). Thus, logging module is capable of tracking information related to IP (Internet Protocol) address information indicative of the virtual location of the browser 200 of Fig. 2, as well as the number of successful hits versus the number of unauthorized and/or unauthenticated requests posted to it by the security module 212 of Fig. 2. With this information, a developer is able to track the number and type of http requests which the servlet processes.(col. 5, lines 8-14). The reference also teaches that by the flags accumulated in the logging module, the servlet programmer/developer can provide the capability of, for example, tracking hackers (both potential and actual) by logging multiple failed accesses by a particular browser within a specific period of time or determine the frequency and type of various security failures promulgated by the user of a particular browser. (col. 4, lines 59-64). Thus, the capability is provided to determine the frequency of the access based on the information contained by logging module for each access regardless whether it is successful (authorized) or failed (unauthorized). The reference fails to teach indicating that the request is unauthorized when the request frequency exceeds a maximum HTTP request frequency. The reference Primeaux teaches a method that will prevent a destructive command from being executed. Several commands for each of the system users are tracked. A combination of security rules and user usage patterns are used to flag suspicious activity on the system. Security rules are centered around those types of

commands that are potentially destructive in nature and take into account the user's normal level of access privileges. (col. 2, lines 45-52). The reference also teaches that the system also may have two or more threshold levels for security monitoring: one for normal operations and any number for heightened security. (teaches to set a threshold level of normal operations such as request count exceeding a maximum HTTP request frequency.)(col.3, lines 21-24). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's logging module's capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request frequency set by the security rules of Primeaux. In this way, a web site owner is able to better track the web site usage as well as be able to determine the number of users which have attempted to enter a particular site and those that have failed and/or succeeded in entering the site in question as taught by Prabandham.

Referring to claim 13,

Claim 13 is a claim to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claim 2. Therefore, claim 13 is rejected for the reasons set forth for the claim 2.

Referring to claims 14, 15 and 16,

Claims 14, 15 and 16 are claims to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of

method of claims 3, 4 and 5. Therefore, claims 14, 15 and 16 are rejected for the reasons set forth for the claims 3, 4 and 5.

Referring to claims 17, 18, 19 and 20,

Claims 17, 18, 19 and 20 are claims to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claims 6, 7, 8 and 9. Therefore, claims 17, 18, 19 and 20 are rejected for the reasons set forth for the claims 6, 7, 8 and 9.

Referring to claims 21 and 22,

Claims 21 and 22 are claims to a program storage device readable by a machine, embodying a program of instructions executable by the machine to perform the steps of method of claims 10 and 11. Therefore, claims 21 and 22 are rejected for the reasons set forth for the claims 10 and 11.

Referring to claim 24,

Claim 24 is a claim to an apparatus carrying out the method of claim 2. Therefore, claim 24 is rejected for the reasons set forth for the claim 2.

Referring to claims 25, 26 and 27,

Claims 25, 26 and 27 are claims to an apparatus carrying out the method of claims 3, 4 and 5. Therefore, claims 25, 26 and 27 are rejected for the reasons set forth for the claims 3, 4 and 5.

Referring to claims 28, 29, 30 and 31,

Claims 28, 29, 30 and 31 are claims to an apparatus carrying out the method of claims 6, 7, 8 and 9. Therefore, claims 28, 29, 30 and 31 are rejected for the reasons set forth for the claims 6, 7, 8 and 9.

Referring to claims 32 and 33,

Claims 32 and 33 are claims to an apparatus carrying out the method of claims 10 and 11. Therefore, claims 32 and 33 are rejected for the reasons set forth for the claims 10 and 11.

Referring to claim 36,

The reference Prabandham teaches HTTP request being made by the subscriber. (Fig. 2, element 202 making http request). The reference also teaches of a servlet engine that includes a security module that assures that only those requests that are properly authenticated and authorized are serviced by a servlet. (a responder to applying HTTP server attack preventative measures). A logging module provides customized records of both security module and servlet transactions (updater that is counting the HTTP requests and updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and.) (Abstract). The reference also teaches that the logging of the servlet transactions provide the capability of, for example, tracking hackers (both potential and actual) by logging multiple failed accesses by a particular browser within a specific period of time or determine the frequency and type of various security failures promulgated by the user of a particular browser. (col. 4, lines 60-64). The reference also teaches that the logging module typically tracks information related to IP (Internet Protocol) address information indicative of the virtual location of the

browser 200 of Fig.2, as well as the number of successful hits versus the number of unauthorized and/or unauthenticated requests posted to it by the security module 212 of Fig. 2. With this information, a developer is able to track the number and type of http requests which the servlet processes. (col. 5, lines 9-16). The reference fails to teach applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count. The reference Primeaux teaches a method that will prevent a destructive command from being executed. Several commands for each of the system users are tracked. A combination of security rules and user usage patterns are used to flag suspicious activity on the system. Security rules are centered around those types of commands that are potentially destructive in nature and take into account the user's normal level of access privileges. (col. 2, lines 45-52). The reference also teaches that the system also may have two or more threshold levels for security monitoring: one for normal operations and any number for heightened security. (teaches to set a threshold level of normal operations such as request count exceeding a maximum HTTP request count.)(col.3, lines 21-24). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's responder 210 containing the logging module with its capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request counts set by the security rules of Primeaux. In this way, a web site owner is able to better track the web site usage as well as be able

to determine the number of users which have attempted to enter a particular site and those that have failed and/or succeeded in entering the site in question as taught by Prabandham.

Referring to claims 37, 38 and 39,

Keeping in mind the teachings of Prabandham as stated above, although the reference teaches the packet switching protocols such as TCP exchanging messages between the subscriber and named host including a server (Fig. 1, col. 1, lines 20-37), the reference fails to teach responder setting an alarm when request count exceeds said maximum HTTP request count and sending alarm to an Internet Service Provider (ISP) associated with subscriber and, dropping the data packet containing request when said request count exceeds maximum HTTP request count. The reference Primeaux teaches the action taken could be defined to suspend the user account or merely mail a message to the system administrator (sending alarm to an Internet Service Provider (ISP) associated with subscriber), warning of a potential intruder including the category of users such as Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (dropping the data packet containing request). Various levels of security are determined by the list of commands deemed critical by the system administrator.(col. 10, lines 60-67). Therefore,

it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's responder 210 containing the logging module with its with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request counts set by the security rules and setting an alarm to the ISP (the system administrator) or dropping a packet containing the request when request count exceeds a maximum HTTP. This provides a system wherein the system will detect a difference in the pattern of command usage. When such a difference is detected, it will be compared to the set of security rules and the system will take the appropriate action.

Referring to claims 40, 41, 42 and 43,

Keeping in mind the teachings of Prabandham as stated above, although the reference teaches the subscriber and the first communication network (Fig.2, elements 202 making http request to element 204), the reference fails to teach the responder shutting down the account used to access first communication network when request count exceeds said maximum HTTP request count and disabling HTTP requests for a hold-down period when request count exceeds maximum HTTP request count. The reference The reference Primeaux teaches the action taken could be defined to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) or merely mail a message to the system administrator, warning of a potential intruder including the category of users such as

Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user.(col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (hold-down period each time HTTP count exceeds said maximum HTTP request count and hold-down period increases exponentially each time HTTP count exceeds maximum HTTP request count). Various levels of security are determined by the list of commands deemed critical by the system administrator.(col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's responder 210 containing the logging module with its capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request counts set by the security rules and to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) as desired, based on the level of security awareness that the software is set for (hold-down period each time HTTP count exceeds said maximum HTTP request count and hold-down period increases exponentially each time HTTP count exceeds maximum HTTP request count) when request count exceeds a maximum HTTP. This provides a system wherein the system will detect a difference in the pattern of command usage. When

such a difference is detected, it will be compared to the set of security rules and the system will take the appropriate action.

Referring to claims 44 and 45,

In addition to the teachings indicated above, the reference Prabandham's servlet handles those requests that are authenticated and authorized by the security module and the servlet notifies the logging module of those requests which have been successfully handled by the servlet with a first type flag. The servlet notifies the logging module of those requests which have not been successfully handled by the servlet with a second type flag. (col.2, lines 53-60). Thus, logging module is capable of tracking information related to IP (Internet Protocol) address information indicative of the virtual location of the browser 200 of Fig. 2, as well as the number of successful hits versus the number of unauthorized and/or unauthenticated requests posted to it by the security module 212 of Fig. 2. With this information, a developer is able to track the number and type of http requests which the servlet processes.(col. 5, lines 8-14). The reference also teaches that by the flags accumulated in the logging module, the servlet programmer/developer can provide the capability of, for example, tracking hackers (both potential and actual) by logging multiple failed accesses by a particular browser within a specific period of time or determine the frequency and type of various security failures promulgated by the user of a particular browser. (col. 4, lines 59-64). Thus, the capability is provided to determine the frequency of the access based on the information contained by logging module for each access whether it is successful (authorized) and failed (unauthorized). The reference fails to teach indicating that the request is

unauthorized when the request frequency exceeds a maximum HTTP request frequency. The reference Primeaux teaches a method that will prevent a destructive command from being executed. Several commands for each of the system users are tracked. A combination of security rules and user usage patterns are used to flag suspicious activity on the system. Security rules are centered around those types of commands that are potentially destructive in nature and take into account the user's normal level of access privileges.(col. 2, lines 45-52). The reference also teaches that the system also may have two or more threshold levels for security monitoring: one for normal operations and any number for heightened security. (teaches to set a threshold level of normal operations such as request count exceeding a maximum HTTP request frequency.)(col.3, lines 21-24). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Prabandham's responder 210 containing the logging module with its capabilities with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as request count exceeding a maximum HTTP request frequency set by the security rules of Primeaux. In this way, a web site owner is able to better track the web site usage as well as be able to determine the number of users which have attempted to enter a particular site and those that have failed and/or succeeded in entering the site in question as taught by Prabandham.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (703) 305-2655. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on (703) 305-8498. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100